IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
EAST BAY

Audit Report 10-34
October 13, 2010

Members, Committee on Audit

Henry Mendoza, Chair
Raymond W. Holdsworth, Vice Chair
Nicole M. Anderson  Margaret Fortune
George G. Gowgani  Melinda Guzman
William Hauck

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
Audit Manager: Greg Dove
Senior Auditor: Eric Wilson

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

Executive Summary ................................................................................................................................. 1

Introduction ............................................................................................................................................. 3
  Background .......................................................................................................................................... 3
  Purpose .............................................................................................................................................. 5
  Scope and Methodology ....................................................................................................................... 7

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Alternate Processing ............................................................................................................................... 8

Backup Procedures ............................................................................................................................... 10

End-User Coordination and Restoration Procedures ............................................................................ 11

Disaster Recovery Planning .................................................................................................................. 13
### APPENDICES

APPENDIX A: Personnel Contacted  
APPENDIX B: Campus Response  
APPENDIX C: Chancellor’s Acceptance

### ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSU</td>
<td>California State University</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>EOC</td>
<td>Emergency Operations Center(s)</td>
</tr>
<tr>
<td>FISMA</td>
<td>Financial Integrity and State Manager’s Accountability Act</td>
</tr>
<tr>
<td>ICSUAM</td>
<td>Integrated California State University Administrative Manual</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Systems</td>
</tr>
<tr>
<td>ITDR</td>
<td>Information Technology Disaster Recovery</td>
</tr>
<tr>
<td>SAM</td>
<td>State Administrative Manual</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2009, the Board of Trustees, at its January 2010 meeting, directed that Information Technology Disaster Recovery (ITDR) be reviewed. The Office of the University Auditor had previously reviewed ITDR for financial systems in the biennial Financial Integrity and State Manager’s Accountability Act (FISMA) and Auxiliary Organization audits.

We visited the California State University, East Bay campus from June 8, 2010, through June 11, 2010, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, would result in significant risk exposures if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: alternate processing, backup procedures, end-user coordination and restoration procedures, and disaster recovery planning. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, due to the effect of the weaknesses described above, the operational and administrative controls of ITDR activities in effect as of June 11, 2010, taken as a whole, were not sufficient to meet the objectives stated in the “Purpose” section of this report.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

ALTERNATE PROCESSING [8]

The campus had not properly managed data storage and hardware replacement vendor contracts and had not tested the designated alternate processing facility for its ability to support the electrical, environmental, and networking demands of such an operation. Further, Information Technology Systems (ITS) had not identified critical systems or prioritized their recovery.

BACKUP PROCEDURES [10]

The campus had not taken appropriate steps to ensure that information systems data would be available in the event of a localized disaster. For example, the campus had not determined how often backup data should be sent off-site for storage, had not ensured that sensitive data was encrypted before transportation to off-site storage, and had not developed methods to ensure access to data processing systems hosted by external vendors in the event of a localized disaster.
END-USER COORDINATION AND RESTORATION PROCEDURES [11]

ITS was unaware of the data processing capabilities expected by end users. Also, business units were unaware of the need for modification of the recovery strategy to enable recovery of data processing services to align with campus-specific time frames, were unaware of their responsibility to provide backup copies of their operating-system and application software, and had not been directed to develop manual processes for critical activities in the event of an extended data processing outage.

DISASTER RECOVERY PLANNING [13]

The campus’ ITDR plan needed further development. For example, the current plan had not been updated recently, did not cross-reference other campus emergency response plans, had not been tested in a disaster recovery simulation, and was not designed in a manner that would allow a competent individual who is unfamiliar with the system to perform recovery activities without extensive guesswork.
INTRODUCTION

BACKGROUND

Information Technology Disaster Recovery (ITDR) planning is a specific subset of an entity’s business continuity planning process that addresses how the IT resources required to operate critical business functions will be restored in a timely and effective manner following a disaster. ITDR planning requires the interaction of individuals at every level of an organization and a recognition by the organization that, in today’s computer-driven work environment, the loss of data processing capabilities can lead to significant financial loss and non-financial exposures if an organization has not planned properly for such an occurrence.

The ITDR planning process requires the evaluation and consideration of several factors, including:

- Who will coordinate the recovery activities, and which supporting groups will report to that coordinator.
- How business units will be impacted if data processing capabilities are lost.
- Which IT systems are critical to support those business units.
- How systems will be restored in the event of a disaster, whether alternate processing facilities will be necessary, whether backup hardware should be stockpiled, and whether insurance coverage will be needed to cover the costs of the recovery activities.
- The kind of training individuals involved with the recovery activities will need to ensure they will be prepared to respond to a disaster in a concise and coordinated manner.
- What incidents have occurred in the past that tested the recovery capabilities of the IT systems, how plans have been modified as a result of the incidents, and what simulated testing is required to refine the effectiveness of the plan.

Because organizational and operational design variances exist between the 23 campuses and the Office of the Chancellor, each campus process must consider many unique factors. Campuses have been directed to prepare ITDR plans for disasters via multiple directives, including, but not limited to, State Administrative Manual (SAM) §5355-5355.2, Executive Order (EO) 1014, and the Integrated California State University Administrative Manual (ICSUAM) §8085.0.

SAM §5355-5355.2 directs state agencies to develop, implement, test, and modify disaster recovery plans, including plans specific to IT assets. SAM §5355 states that agencies must take appropriate steps to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure that essential business functions will continue in the event of a disaster. SAM §5355.1 states that, in developing an ITDR plan, agencies should provide for the continuity of computing operations in support of critical business functions, minimize the need for decision-making during a disaster and subsequent recovery, and plan for the migration of computing resources toward resumption of operational capacity in an expeditious and efficient manner. In preparing such a plan, SAM §5355.1 directs that ongoing testing, analysis, and modification of plan assumptions and activities must occur. SAM §5355.2 states that each
agency must maintain a list of computer applications that are critical to agency operations, information assets required by such applications, and a method by which such applications will be reestablished.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, provides detailed guidance to campuses for creating, implementing, and maintaining a business continuity program that includes an ITDR plan. EO 1014 states that goals, which must be met by such a program, include, but are not limited to:

- Maintaining a program on each campus that ensures the continuity of essential functions or operations following a catastrophic event.
- Establishing recovery goals and objectives for the campus that reflect the needs of the campus and its business units.
- Identifying functions and assets that are essential to the operational continuity needed to support the campus’ mission.
- Recommending recovery strategies based on the circumstances of various events.
- Listing, prioritizing, and establishing recovery time objectives for essential functions, systems, and applications through business impact analyses and risk assessments.
- Establishing and testing alternate data processing capabilities, if deemed necessary.
- Protecting and safeguarding vital database systems and data assets.
- Reviewing, testing, modifying, and validating recovery plans in terms of campus and business unit expectations.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, represents the most recent and specific guidance to campuses in regard to ITDR planning. Simply stated, the policy directs campuses to ensure that information assets can continue to operate or, in a reasonable time frame, be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster or other emergency event. While the policy itself does not provide detailed operational requirements, it can be surmised that the campuses must consider a multitude of factors such as restart times, backup and recovery procedures, system security (environmental, physical, and logical), and system interdependence and redundancy to ensure a satisfactory level of continued operational capacity.
Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to ITDR planning and to determine the adequacy of controls that ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the audit objective, specific goals included determining whether:

- The administration of the ITDR program incorporates a defined mission, stated goals and objectives, and clear lines of organizational authority and responsibility, and is adequately funded.
- The ITDR plan is reviewed and modified on a regular basis, and modifications reflect the needs of the campus and the business units.
- Adequate system redundancy or alternate processes exist to ensure minimal interruption of critical business services.
- System backups and record retention are sufficient to meet the recovery objectives of the campus.
- Initiatives and investments are underway to improve ITDR planning and maximize ITDR resources; risks specific to the campus have been identified; and policies and procedures are current, comprehensive, and sufficient to support campus ITDR planning.
- An adequate emergency operations center (EOC) exists; sufficient equipment, supplies, and other critical resources are properly provisioned; and the campus is fully prepared for emergencies affecting data processing activities.
- The ITDR plan clearly identifies who has authority and responsibility for emergencies and incidents, and the emergency organization is sufficient to ensure that campus command/incident command techniques provide command and control when emergency incidents occur.
- ITDR resources are available; plans have been updated appropriately; and plans are integrated with the campus business continuity plan.
- Previous incidents were mitigated in a timely manner; lessons learned were evaluated; appropriate after-action reports were prepared; and sufficient plans for mitigation of any such incidents in the future are in place.
- Simulated tests of plan components are routinely scheduled, and after-action reports and modifications are generated.
- The potential outage times expected while executing the ITDR plan have been adequately communicated to and coordinated with the campus community, and emergency communications and operations are adequately coordinated and managed.
The campus business units have taken an active role in determining the prioritization of systems and their recovery time expectations.

Sufficient training has been provided to employees, disaster recovery staff, and building marshals who are expected to execute the ITDR plan, and the finance function has been integrated into the disaster recovery activities.

The ITDR plan is written so that a competent individual or group of individuals who are unfamiliar with the campus’ systems would be able to execute a portion or all of the recovery steps if needed.
SCOPe AND METHODOLOGY

The proposed scope of this audit was presented in Attachment A of Audit Agenda Item 2 during the January 26 and 27, 2010, meeting of the Committee on Audit. The attachment stated that the ITDR audit would include a review of Trustee policy, systemwide directives, campus policies and procedures, the essential functions or operations following a catastrophic event, business impact analysis and risk assessment, business continuity and disaster recovery plans, testing and exercising of plans, plan maintenance, communications, training, and necessary retention of key records.

The scope of this audit is focused on the campus’ ITDR planning specific to a disaster only affecting data processing services.

Our study and evaluation was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures in effect during fiscal year 2009/10. In instances wherein it was necessary to review annualized data, calendar years 2009 and 2010 were the periods reviewed.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

- The ITDR planning management organization.
- The ITDR plan for all critical campus data processing activities.
- Disaster recovery plan guidelines, policies, procedures, and recordkeeping.
- The building marshal program, emergency action plans, and campus emergency hotline, as it relates to IT disasters.
- The EOC, emergency equipment, and related emergency supplies applicable to ITDR.
- Coordination with other agencies and vendors, including mutual aid and assistance.
- Funding and budgetary controls for disaster recovery planning activities.
- Communication of the disaster recovery plan.
- Training for emergency activities affecting data processing.
- Evacuation drills and emergency plan testing affecting campus data processing facilities.
- Backup and retention of system data.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

ALTERNATE PROCESSING

Campus planning for restoration of processing capabilities after a disaster needed improvement.

We found that:

- The contract with the off-site data storage vendor for backup tapes expired in 2009.

- Although the campus’ Emergency Operations Center (EOC) had been designated as the alternate processing center in the event of a disaster, the EOC’s capacity to support the electrical, environmental, and telecommunications demands of such an operation had not been tested.

- Information Technology Systems (ITS) had not designated which IT systems are critical to the operation of the campus and had not determined the order in which such systems should be reactivated in the event of a disaster affecting the data center.

- ITS had not prioritized or vetted the equipment list that was provided to the replacement vendor, and several pieces of equipment would not need to be on the contract for immediate replacement.

- The campus had not formally determined if it would accept replacement equipment on a lease or purchase basis from the vendor, which is a contractual requirement for delivery. In addition, the terms of leasing the equipment had not been clarified.

California State University Policy Manual for Contracting and Procurement, dated October 5, 2007, states that the campuses must enter into contracts with all service providers and that the contracts must contain specific protections for the campus and the California State University (CSU).

Executive Order (EO) 1014, California State University Business Continuity Plan, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

State Administrative Manual (SAM) §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems that are critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.

Integrated California State University Administrative Manual (ICSUAM) §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that critical business services are restored with minimal interruption in the event of a disaster.
The director of server and network operations stated that these conditions were the result of operational oversight. He further stated that the lapse in the current vendor agreement and lack of defined terms for accepting replacement equipment were the result of administrative oversight.

Failure to properly develop alternate processing capabilities can result in both financial and non-financial losses to the campus and the CSU and can result in unexpected delays in the recovery of data processing services.

**Recommendation 1**

We recommend that the campus:

a. Execute a current agreement with the off-site backup media storage vendor.

b. Determine the specific requirements for operating the campus data center from the EOC.

c. Identify critical systems and prioritize their recovery.

d. Determine which equipment would need to be immediately replaced in the event of a disaster affecting the data center.

e. Determine the method in which equipment will be accepted from the replacement vendor and clarify the terms for leasing such equipment.

**Campus Response**

We concur.

a. An agreement with the off-site backup media storage vendor will be executed by November 30, 2010.

b. The campus will determine specific requirements for operating the campus data center from the EOC by November 30, 2010.

c. Critical systems will be identified and their recovery shall be prioritized by November 30, 2010.

d. The campus will determine which equipment would need immediate replacement in the event of a disaster affecting the data center by November 30, 2010.

e. The campus will notify the replacement vendor by November 30, 2010, that we will lease the equipment once delivered, and not exercise the option to purchase.
BACKUP PROCEDURES

ITS had not adequately ensured that information systems data would be available in the event of a localized disaster.

We reviewed the campus’ data backup processes and system redundancy designs and found that:

- A process had not been developed for the transfer of backup media off-site based on the determination of the appropriate amount of data loss that would be acceptable to business units.
- Sensitive data was not encrypted before it was transferred to off-site storage.
- Network authentication redundancy had not been developed to allow users access to critical applications, such as PeopleSoft, if an event adversely affects the data center.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

SAM §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems that are critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.

ICSUAM §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that critical business services are restored with minimal interruption in the event of a disaster.

EO 1014, California State University Business Continuity Plan, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

The director of server and network operations stated that not physically removing the backup media from the data center on a regular basis and not creating redundancy in the authentication system was the result of improper planning. He further stated that data was not encrypted during the backup process because the campus had not clearly defined who was responsible for such activities, ITS or the data owners.

Failure to protect sensitive data, ensure that the potential for data loss is minimized, and develop processes to minimize disruptions to data processing capabilities exposes the campus and the CSU to legal and financial damages.
Recommendation 2

We recommend that the campus:

a. Develop a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

b. Ensure that all sensitive data is encrypted before being sent off-site.

c. Develop network authentication redundancy so users can access critical applications such as PeopleSoft if an event adversely affects the data center.

Campus Response

We concur.

a. By November 30, 2010, the campus will develop a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

b. By November 30, 2010, the campus will ensure that all sensitive data is encrypted before being sent off-site.

c. The campus will begin to develop network authentication redundancy so users can access critical applications if an event adversely affects the data center by November 30, 2010. The process will be completed by March 31, 2011.

END-USER COORDINATION AND RESTORATION PROCEDURES

IT recovery expectations had not been clearly communicated to ITS and business-end users.

Specifically, we found that:

- Because a campus-wide end-user impact analysis had not been performed, ITS was unaware of the recovery expectations of the various business units.

- The recovery strategy required modification to enable recovery of data processing services to align with campus-specific time frames and was not communicated to the business units.

- Business units had not been informed of their responsibility to provide backup copies of operating-system and application software, as ITS only backed up data from the campus servers.

- Business units had not communicated their plans to ITS to process data manually during an extended data processing outage, to verify the state of data upon recovery, and to determine what data must be re-created from alternative sources.
SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, states that the campus shall have each critical business unit perform a business impact assessment to determine the financial and non-financial losses associated with, among other items, a loss of data processing capabilities.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that critical business services are restored with minimal interruption in the event of a disaster.

The director of server and network operations stated that the lack of communication between the business units and ITS occurred because such communications had not been prioritized previously. The vice president of administration and finance stated that his division had performed a business impact analysis but was unaware of whether other divisions had performed such an analysis. He further stated that he was unaware if manual processes and data verification methods had been communicated to the other divisions.

Failure to understand the needs of the critical business units and failure to communicate potential outage times and other recovery requirements to end users increases the likelihood that the campus will be unprepared to respond to a localized disaster and could significantly impact the campus’ ability to recover data processing services.

**Recommendation 3**

We recommend that the campus:

a. Perform a campus-wide business impact analysis to determine which business units are critical and what the acceptable time frames for data processing outage are for each.

b. Modify the recovery strategy to enable recovery of data processing services to align with campus-specified time frames.

c. Inform the various business units of their responsibility to provide backup copies of operating-system and application software.

d. Direct the various business units to communicate their plans to ITS to process data manually during an extended data processing outage, to verify the state of data upon recovery, and to determine what data must be re-created from alternative sources.
Campus Response

We concur.

a. We will perform a campus-wide business impact analysis. The outcome will be to identify mission-critical business units and to determine acceptable time frames for data processing outages. This analysis will be completed by March 31, 2011.

b. Based on the results of the campus-wide business impact analysis, we will modify our data processing recovery strategy to ensure it is aligned with the business needs by March 31, 2011.

c. We will inform each university division of its responsibility to maintain backup copies of operating-system and application software by December 31, 2010.

d. We will direct each university division to communicate to ITS its plans to manually process data during an extended data processing outage. This plan shall include how the unit will verify the state of the data upon recovery and determine what data must be recovered from alternative sources. This will be completed by April 30, 2011.

DISASTER RECOVERY PLANNING

The campus’ ITDR plan needed further development.

We found that the current ITDR plan:

- Had not been updated since 2008 and included systems that had been retired from service.
- Did not cross-reference other campus emergency response plans.
- Did not provide a step-by-step process detailing who, what, when, where, and how the plan should be executed immediately preceding, during, and following an emergency event.
- Did not include instructions for ensuring that alarms had not been triggered by a false sensor reading, failed equipment, or other malfunction.
- Had not been tested in a simulated disaster recovery.
- Did not include sufficient detail to allow a competent individual who is not directly familiar with each campus system to recover the application systems and hardware without undue delay, research, and/or guesswork.

SAM §5355.1 states that a disaster recovery plan should be designed such that the requirement for decision-making during and after an event is minimized and individuals are provided direction in as clear and concise a manner as possible. Also, disaster recovery plans must be viable, fully documented, and tested.
EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, states that the campus must keep all business continuity-related plans current, must test all plans for viability, and must reference all materials necessary to recover from a disaster.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, says, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that critical business services are restored with minimal interruption in the event of a disaster.

The director of server and network operations stated that not having a current, tested, and easily executable disaster recovery plan was the result of administrative oversight. He further stated that not developing the plan in coordination with other campus personnel involved in disaster recovery and business continuity activities was the result of not having a clear campus-wide mandate to do so.

Failure to maintain a current, tested, and easily executable disaster recovery plan can result in unnecessary financial and non-financial losses in the event of a disaster and could significantly impact the campus’ ability to recovery from a disaster affecting data processing services.

**Recommendation 4**

We recommend that the campus:

a. Update the ITDR plan to include current systems and insert cross-references to other campus emergency response plans that would be pertinent to a systematic recovery of data processing capabilities.

b. Update the ITDR plan to clarify each individual’s role in the recovery process.

c. Update the ITDR to include instructions for determining whether alarms had been triggered by malfunctions such as false sensor readings and failed equipment, etc.

d. Test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results.

e. Update the ITDR to include sufficient detail to allow an individual not directly familiar with each campus system to recover application systems and hardware without undue delay, research, and/or guesswork.

**Campus Response**

We concur.

a. The campus will update the ITDR plan by November 30, 2010, to include the current systems and insert cross-references to other campus emergency plans.
b. The campus will update the ITDR plan by November 30, 2010, to clarify each functional role within the recovery process and include an appendix that identifies the individuals assigned to each functional role.

c. The campus will update the ITDR plan by November 30, 2010, to include instructions for determining whether alarms had been triggered by malfunctions such as false sensor readings and failed equipment, etc.

d. The campus will test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results by November 30, 2010.

e. The campus will create a disaster recovery checklist by November 30, 2010, that will allow individuals who are not familiar with each campus system to recover application systems and hardware.
### APPENDIX A:
**PERSONNEL CONTACTED**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mohammad H. Qayoumi</td>
<td>President</td>
</tr>
<tr>
<td>Rich Avila</td>
<td>Director, Server and Network Operations</td>
</tr>
<tr>
<td>Shawn Bibb</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Lee Breitzman</td>
<td>Lead Operations Specialist, Server Operations</td>
</tr>
<tr>
<td>John Charles</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Matt Collins</td>
<td>Director, Application Systems</td>
</tr>
<tr>
<td>Chris Da Silva</td>
<td>Network Analyst</td>
</tr>
<tr>
<td>Thomas Dixon</td>
<td>Network Security Analyst</td>
</tr>
</tbody>
</table>
December 2, 2010

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802

RE: Campus Responses to Recommendations: Audit Report Number 10-34
IT Disaster Recovery, California State University, East Bay

Dear Mr. Mandel,

Enclosed is our response to the recommendations in Audit Report Number 10-34, IT Disaster Recovery Audit, at California State University, East Bay.

Upon acceptance of our response, we will follow up with your office, providing supporting documentation for the recommendations.

Please let us know if you have any questions or need additional information.

Sincerely,

Shawn Bibb
Vice President, Administration & Finance, CFO

cc: Mohammad H. Qayoumi, President
John Charles, CIO
Lee Thompson, Deputy CIO
IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
EAST BAY

Audit Report 10-34

ALTERNATE PROCESSING

Recommendation 1

We recommend that the campus:

a. Execute a current agreement with the off-site backup media storage vendor.

b. Determine the specific requirements for operating the campus data center from the EOC.

c. Identify critical systems and prioritize their recovery.

d. Determine which equipment would need to be immediately replaced in the event of a disaster affecting the data center.

e. Determine the method in which equipment will be accepted from the replacement vendor and clarify the terms for leasing such equipment.

Campus Response

We concur.

a. An agreement with the off-site backup media storage vendor will be executed by November 30, 2010.

b. The campus will determine specific requirements for operating the campus data center from the EOC by November 30, 2010.

c. Critical systems will be identified and their recovery shall be prioritized by November 30, 2010.

d. The campus will determine which equipment would need immediate replacement in the event of a disaster affecting the data center by November 30, 2010.

e. The campus will notify the replacement vendor by November 30, 2010, that we will lease the equipment once delivered, and not exercise the option to purchase.
BACKUP PROCEDURES

Recommendation 2

We recommend that the campus:

a. Develop a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

b. Ensure that all sensitive data is encrypted before being sent off-site.

c. Develop network authentication redundancy so users can access critical applications such as PeopleSoft if an event adversely affects the data center.

Campus Response

We concur.

a. By November 30, 2010, the campus will develop a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

b. By November 30, 2010, the campus will ensure that all sensitive data is encrypted before being sent off-site.

c. The campus will begin to develop network authentication redundancy so users can access critical applications if an event adversely affects the data center by November 30, 2010. The process will be completed by March 31, 2011.

END-USER COORDINATION AND RESTORATION PROCEDURES

Recommendation 3

We recommend that the campus:

a. Perform a campus-wide business impact analysis to determine which business units are critical and what the acceptable time frames for data processing outage are for each.

b. Modify the recovery strategy to enable recovery of data processing services to align with campus-specified time frames.

c. Inform the various business units of their responsibility to provide backup copies of operating-system and application software.

d. Direct the various business units to communicate their plans to ITS to process data manually during an extended data processing outage, to verify the state of data upon recovery, and to determine what data must be re-created from alternative sources.
Campus Response

We concur.

a. We will perform a campus-wide business impact analysis. The outcome will be to identify mission critical business units and to determine acceptable timeframes for data processing outages. This analysis will be completed by March 31, 2011.

b. Based on the results of the campus-wide business impact analysis, we will modify our data processing recovery strategy to ensure it is aligned with the business needs by March 31, 2011.

c. We will inform each university division of its responsibility to maintain backup copies of operating system and application software by December 31, 2010.

d. We will direct each university division to communicate to ITS its plans to manually process data during an extended data processing outage. This plan shall include how the unit will verify the state of the data upon recovery and to determine what data must be recovered from alternative sources. This will be completed by April 30, 2011.

DISASTER RECOVERY PLANNING

Recommendation 4

We recommend that the campus:

a. Update the ITDR plan to include current systems and insert cross-references to other campus emergency response plans that would be pertinent to a systematic recovery of data processing capabilities.

b. Update the ITDR plan to clarify each individual’s role in the recovery process.

c. Update the ITDR to include instructions for determining whether alarms had been triggered by malfunctions such as false sensor readings and failed equipment, etc.

d. Test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results.

e. Update the ITDR to include sufficient detail to allow an individual not directly familiar with each campus system to recover application systems and hardware without undue delay, research, and/or guesswork.

Campus Response

We concur.

a. The campus will update the ITDR plan by November 30, 2010, to include the current systems and inserted cross-references to other campus emergency plans.
b. The campus will update the ITDR plan by November 30, 2010, to clarify each functional role within the recovery process and it includes an appendix that identifies the individuals assigned to each functional role.

c. The campus will update the ITDR plan by November 30, 2010, to include instructions for determining whether alarms had been triggered by malfunctions such as false sensor readings and failed equipment, etc.

d. The campus will test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results by November 30, 2010.

e. The campus will create a disaster recovery checklist by November 30, 2010, that will allow individuals, who are not familiar with each campus system, to recover application systems and hardware.
December 15, 2010

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
       Chancellor

SUBJECT: Draft Final Report 10-34 on IT Disaster Recovery,
         California State University, East Bay

In response to your memorandum of December 15, 2010, I accept the response
as submitted with the draft final report on IT Disaster Recovery, California
State University, East Bay.

CBR/amd